

Módulo Configuration Protection

Para proteger su información valiosa de cualquier pérdida (accidental o maliciosa), su solución de seguridad deberá cubrir la protección de los dispositivos de almacenamiento extraíbles, las interfaces físicas e inalámbricas, y los usuarios. SafeGuard Configuration Protection controla y protege las estaciones de trabajo y los dispositivos en todas las interfaces, y garantiza una prevención contra fugas de datos flexible y fácil de usar.

Mayor seguridad

- Impide filtraciones y robos de datos, ataques en la empresa e introducción de malware
- El control granular detecta y limita la transferencia de datos por tipo y modelo de dispositivo, número de serie único y tipo de archivo
- Protege los datos de la empresa almacenados en dispositivos externos durante desplazamientos del usuario y controla el uso fuera de Internet
- Bloquea los registros de pulsaciones en el teclados tanto USB como PS/2
- Limita la función U3 (ejecución automática) para los medios extraíbles
- El agente de seguridad impide la violación de las políticas de seguridad: despliegue silencioso, redundante y prevención contra manipulaciones a varios niveles

Funciones de seguridad: control del uso

- Puertos: permite/bloquea su uso
- Dispositivos y medios de almacenamiento: listas de exclusión según el tipo, modelo y número de serie
- Control de solo lectura o lectura/escritura para medios de almacenamiento portátiles
- Bloquea los registros de pulsaciones en teclados tanto USB como PS/2
- Archivos: limita las transferencias según el tipo de archivo
- Wi-Fi: listas de exclusión según SSID
- Bloquea los puentes híbridos de red

Auditoría del estado de seguridad de la estación de trabajo

- Visibilidad integral de las conexiones a las estaciones de trabajo corporativas
- Visibilidad de todos los puertos USB, PCMCIA, FireWire y Wi-Fi
- Registro granular de el historial de todas las conexiones a un dispositivo
- Informes sencillos y efectivos

Potente administración central

Ventajas clave

Seguridad mejorada del sistema

- » Controla el tráfico en tiempo real y aplica políticas de seguridad personalizadas y granulares para todo tipo de interfaces y dispositivos de almacenamiento externo como:
 - » Interfaces físicas: USB, FireWire, PCMCIA, puertos paralelos, puertos de serie, etc.
 - » Interfaces inalámbricas: Wi-Fi, Bluetooth, Infrarrojos (IrDA)
 - » Dispositivos de almacenamiento externo: medios extraíbles, CD/DVD, disquetes, etc.
- » Controla el acceso de lectura y escritura basado en grupos de tipos de archivo

La facilidad de uso y las funciones de gestión permiten a los administradores:

- » Detectar y autorizar restricciones de tipos de dispositivos, modelos e incluso números de serie específicos
- » Bloquear completamente todos los dispositivos de almacenamiento
- » Visualizar las conexiones a estaciones corporativas con la herramienta SafeGuard PortAuditor
- » Despliega políticas de seguridad que satisfagan las necesidades empresariales

Mayor productividad y facilidad de uso

- » Sin necesidad de cambios en los hábitos de trabajo de los usuarios
- » Alto nivel de aceptación por parte de los usuarios, ya que no se necesita formación adicional
- » Mayor estabilidad del sistema, gracias a la prevención de unidades y dispositivos no deseados

- La flexibilidad de gestión permite definir políticas separadas por dominio, grupo, ordenador o usuario.
- La información del usuario/ordenador se importa mediante la integración con los servicios de directorio (p.ej.: Microsoft Active Directory).
- Aplicación de políticas avanzadas a través del análisis independiente, a nivel de kernel y en tiempo real, del tráfico de puertos de bajo nivel.
- Los dispositivos que no se hayan comunicado con el centro de administración en períodos determinados de tiempo, pueden bloquearse o cerrarse según la política establecida, mientras estén en la red.
- Los protocolos avanzados XML/SOAP permiten la comunicación con el SafeGuard Management Center.
- Todas las actividades/estados de los clientes y eventos de seguridad se registran y almacenan de forma local y central. Los tipos de registros y la ubicación del almacenamiento están definidos por el usuario. Los administradores pueden filtrar, ver, imprimir y exportar registros e informes con la consola SafeGuard Management Center*.

Instalación fácil y administrada de forma centralizada

- Los paquetes de instalación se pueden distribuir e instalar de forma centralizada y sin supervisión mediante los paquetes MSI estándar.
- La distribución en la red no requiere la participación del usuario.

* Para la administración central, es necesario el módulo SafeGuard Enterprise Management Center. Visite <http://esp.sophos.com>, si desea obtener más información.

Requisitos del sistema

Sistemas operativos

- » Microsoft Windows 7 (de 32 y 64 bits)
- » Microsoft Windows Vista (32 bits; SP 1 y 2)
- » Microsoft Windows XP (32 bits; SP 2 y SP 3)

Requisitos del producto

- » SafeGuard Management Center

Certificaciones

- » Common Criteria EAL 2

Idiomas

- » Español, inglés, francés, alemán, italiano y japonés
- » Compatibilidad de unicode para sistemas operativos en otros idiomas

Resumen del control de puertos

Interfaces físicas

- » USB
- » FireWire
- » PCMCIA
- » Secure Digital (SD)
- » Paralelo
- » Serie
- » Módem

Interfaces inalámbricas

- » Wi-Fi
- » Bluetooth
- » Infrarrojos (IrDA)

Dispositivos de almacenamiento

- » Dispositivos de almacenamiento extraíbles
- » Discos duros externos
- » Unidades de CD/DVD
- » Unidades de disquete
- » Unidades de cinta